

Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof

Dong Yang, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, Wei Song

Abstract—New measures of multipartite entanglement are constructed based on two definitions of multipartite information and different methods of optimizing over extensions of the states. One is a generalization of the squashed entanglement where one takes the mutual information of parties conditioned on the state's extension and takes the infimum over such extensions. Additivity of the multipartite squashed entanglement is proved for both versions of the multipartite information which turn out to be related. The second one is based on taking classical extensions. This scheme is generalized, which enables to construct measures of entanglement based on the *mixed convex roof* of a quantity, which in contrast to the standard convex roof method involves optimization over all decompositions of a density matrix rather than just the decompositions into pure states. As one of the possible applications of these results we prove that any multipartite monotone is an upper bound on the amount of multipartite distillable key. The findings are finally related to analogous results in classical key agreement.

Index Terms—Squashed entanglement, c-squashed entanglement, Mixed convex roof, Multipartite distillable key

I. INTRODUCTION

Many bipartite entanglement measures are known, but few are known for multipartite states. Among the known bipartite entanglement measures, the *squashed entanglement* is distinct from other measures in its additivity and interesting construction [1], [2]. It is based on quantum conditioning. In general, we do not know how to condition upon a quantum register. However if a function is built out of entropies, then there is a more or less magic way of conditioning, which is based on the fact that, accidentally, conditioning classical entropies can be represented by subtracting the conditioning entropy from

the joint entropy – the entropy of the state on A conditioned by the state on B can be written formally as

$$S(A|B) = S(AB) - S(B). \quad (1)$$

Quantum conditional entropy often takes negative values. However, squashed entanglement is built out of the quantum mutual information, which remains positive upon conditioning. The definition of squashed entanglement is inspired by the intrinsic information, a quantity used in classical cryptography.

Interestingly, no multipartite generalization of this measure was proposed so far. In this paper we propose two generalizations, based on two versions of the multiparty mutual information. One of these mutual information generalizations was considered already in [3], [4], while the second one, a kind of dual to the latter, was introduced in [5]. The authors considered both generalizations of mutual information to multipartite setting as so-called secrecy monotones. Thus it is natural to use both to generalize squashed entanglement. We prove that our multipartite versions of squashed entanglement are additive.

In the definition of bipartite squashed entanglement [2], one considers conditional mutual information over extensions of the original state ρ_{AB} to a third system E . We do the same in the multipartite case. The conditioning here is *quantum*: the system E is a quantum register that means the extension state is quantum-correlated between AB and E . This kind of conditioning is applicable only to linear combinations of quantum entropies.

On the contrary, we know how to condition *any* function upon a *classical* register E . Here a question arises: *for which functions, can we obtain a measure of entanglement based on classical conditioning?* In this paper we also attempt to answer this question and show that if the function f satisfies the following conditions

- i) f is invariant under local unitary transformations
- ii) f does not increase under local measurement on average

then, via conditioning, it gives rise to an entanglement measure. The measure turns out to be of similar construction to the convex roof [6], where one optimizes over all pure decompositions of a given state. Here we instead consider decompositions into mixed states (see e.g. [7], [8], [9]),

$$E(\rho) = \inf_{\sum_i p_i \rho_i = \rho} \sum_i p_i f(\rho_i). \quad (2)$$

Such a construction is called the *mixed convex roof*. This approach works in both bipartite as well as the multipartite

Dong Yang was at the Laboratory for Quantum Information, China Jiliang University, Hangzhou, Zhejiang 310018, China.(e-mail:dyang@cjl.u.edu.cn)

Karol Horodecki was at the Faculty of Mathematics, Physics and Computer Science, University of Gdańsk, 80–952 Gdańsk, Poland.(e-mail:khorocec@inf.univ.gda.pl)

Michał Horodecki was at the Institute of Theoretical Physics and Astrophysics University of Gdańsk, 80–952 Gdańsk, Poland.(e-mail:fizmh@univ.gda.pl)

Paweł Horodecki was at the Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80–952 Gdańsk, Poland.(e-mail:pawel@mifgate.pg.gda.pl)

Jonathan Oppenheim was at the Department of Applied Mathematics and Theoretical Physics, University of Cambridge, U.K.(e-mail:J.Oppenheim@damtp.cam.ac.uk)

Wei Song was at the Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China.(e-mail:wsong1@mail.ustc.edu.cn)

We acknowledge support from EU grants IP QAP IST-015848 and IP SCALA IST-015714. J.O. also acknowledges the Royal Society. K.H. acknowledges the support of the Foundation for Polish Science. D.Y. acknowledges the support from NSF of China (Grant No. 10805043).

tite scenario. If the function is the mutual information, we have then two measures, the original squashed entanglement (*q-squashed* entanglement) and the classical squashed (*c-squashed*) entanglement. It should be mentioned that for bipartite systems the latter measure was already considered in [1] as an interpolation between entanglement of formation and squashed entanglement. It was also independently proposed in [7], [10], however, monotonicity of this measure was not proved. Within our approach, the c-squashed entanglement is a special case of mixed convex roof measures, hence it is monotonous.

We also discuss asymptotic continuity of our entanglement measures. In particular, multipartite squashed entanglement is shown to satisfy this condition, which comes from the Alicki-Fannes result [11] (cf. [2]). On the other hand the measures based on mixed convex roof inherit the asymptotic continuity from the original functions [8].

The rest of the paper is organized as follows. Section II briefly recalls the construction of bipartite squashed entanglement. Section III discusses two formulas of multipartite mutual information, then defines their conditional versions and explores their properties. Section IV presents two multipartite entanglement measures. One is the q-squashed entanglement that is based on conditioning on a quantum register, which is the generalization of bipartite squashed entanglement. We consider two versions of q-squashed entanglement, based on two different formulas of multipartite mutual information. We prove additivity for both versions. The other entanglement measure is the c-squashed entanglement that uses conditioning on a classical register. It can also be obtained via the mixed convex roof. Asymptotic continuity is also discussed. In Section V, we show that any multipartite monotone that satisfies reasonable axioms is an upper bound on distillable key, providing q-squashed entanglement as an example. It is a direct generalization of a bipartite result given in [12], based on the multipartite key distillation protocol given in [13]. In Section V-D we consider the classical analogue of the latter fact, that has been already presented in [5]. We consider here more carefully the issue of asymptotic continuity and the presence of the eavesdropper. Section VI provides a summary.

II. BIPARTITE SQUASHED ENTANGLEMENT

In this section, we briefly recall the definition and properties of the original squashed entanglement. It is based on a simple quantity - the quantum mutual information,

$$I(A : B) = S(A) + S(B) - S(AB), \quad (3)$$

where $S(X)$ is the von Neumann entropy of system X . Then one defines the conditional mutual information as

$$I(A : B|E) = S(AE) + S(BE) - S(ABE) - S(E), \quad (4)$$

by simple application of the definition Eq. (1) to the mutual information. The entanglement measure is then obtained by “squashing”.

Definition 1 For a given state ρ_{AB} , squashed entanglement is given by

$$E_{sq}(\rho_{AB}) = \frac{1}{2} \inf I(A : B|E), \quad (5)$$

where the infimum is taken over all extensions ρ_{ABE} of the original state.

The factor $1/2$ is taken just for convenience and an extension is any joint state ρ_{ABE} such that tracing out the state on E leaves ρ_{AB} on AB .

Squashed entanglement satisfies not only the basic properties of entanglement measures - monotonicity under local operations and classical communication (LOCC), but also other useful properties, notably additivity. It is also a good upper bound for distillable entanglement.

III. CONDITIONAL MULTIPARTITE MUTUAL INFORMATION

In this section, we discuss the mutual information for multipartite states and then study the properties of conditional multipartite mutual information.

There are at least two candidates for multipartite mutual information. One is more in the spirit of the Venn diagram representation of information-theoretic identities [14], where the bipartite mutual information corresponds to the intersection of two sets. To extend this notion to the multipartite case, we would need to take the intersection of all sets. For example in the tripartite case this approach would give the following candidate for mutual information

$$S(A) + S(B) + S(C) - S(AB) - S(AC) - S(BC) + S(ABC). \quad (6)$$

This function can however be negative. The other approach, which produces a much simpler function, is to notice that mutual information is the relative entropy between the state and its marginal

$$I(\rho_{AB}) = S(\rho_{AB} || \rho_A \otimes \rho_B), \quad (7)$$

where the relative entropy is defined as

$$S(\rho || \sigma) = \text{tr} \rho (\log \rho - \log \sigma). \quad (8)$$

Thus multipartite mutual information would be

$$I(A : B : C) = S(\rho_{ABC} || \rho_A \otimes \rho_B \otimes \rho_C). \quad (9)$$

This turns out to be a very simple function considered by Lindblad [3] and used in [4] to describe correlations within multipartite quantum systems:

$$I(A_1 : A_2 : \dots : A_m) = \sum_{i=1}^m S(A_i) - S(A_1 A_2 \dots A_m). \quad (10)$$

In this paper we will adopt this function as one measure of multipartite mutual information. Since it can be represented as the relative entropy between a state and the product of its marginals, it is a monotone under local operations (because of the monotonicity of relative entropy [15], [16]).

This version of multipartite mutual information has yet another interesting feature [5]: it can be represented as a sum of bipartite mutual information

$$I(A_1 : A_2 : \dots : A_m) = I(A_1 : A_2) + I(A_3 : A_1 A_2) + I(A_4 : A_1 A_2 A_3) + \dots + I(A_m : A_1 A_2 \dots A_{m-1}). \quad (11)$$

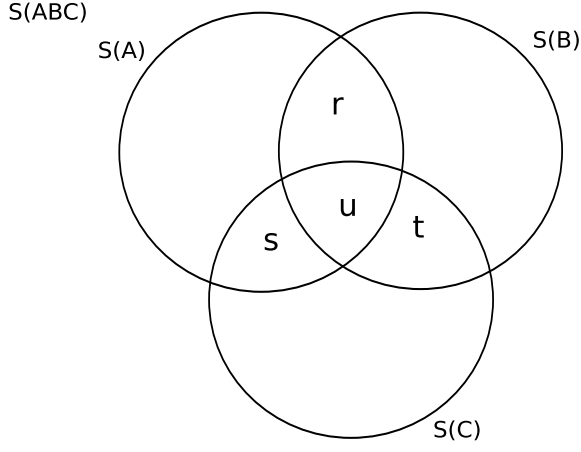


Fig. 1. A graphical representation of entropic quantities for the case of three parties. Here, the region that represents $I(A : B)$ is $r + u$. $S_3 = r + s + t + u$ and $I(A : B : C) = r + s + t + 2u$

Put in a different way, I satisfies the recurrence relation

$$I(A_1 : A_2 : \dots : A_m) = I(A_1 : A_2 : \dots : A_{m-1}) + I(A_m : A_1 \dots A_{m-1}). \quad (12)$$

So it is actually a very simple quantity, which is built as follows: first we consider the (original) mutual information between two chosen parties. Then we want to take into account the next party, so we take the mutual information between it and the previous two parties. In general, to take into account a new party means to add the mutual information between this party and all the other ones (treated jointly). Moreover this quantity is independent of the selected order in which we combine them. It is also obvious that the expression is invariant under permutation of the systems. The fact that multipartite mutual information can be decomposed into bipartite mutual information already indicates that most of the proofs for the original mutual information in the bipartite case can be applied to multipartite case without great modification.

There is yet another formula for mutual information in the multipartite case, as proposed in [5], where multipartite *secrecy monotones* were considered. It is of the form

$$S_m = \sum_{i=1}^m S(\rho_{A_1, \dots, A_{i-1}, A_{i+1}, \dots, A_m}) - (m-1)S(\rho_{A_1 \dots A_m}). \quad (13)$$

It has an alternative expression in terms of conditional mutual information [5] (cf. Eq. 11):

$$\begin{aligned} S_m &= I(A_1 : A_2 \dots A_m) + I(A_2 : A_3 \dots A_m | A_1) \\ &\quad + I(A_3 : A_4 \dots A_m | A_1 A_2) + \dots \\ &\quad + I(A_{m-1} : A_m | A_1 \dots A_{m-2}). \end{aligned} \quad (14)$$

It turns out that the two candidates for mutual information, I and S_m are dual to each other:

$$\begin{aligned} &S_m + I(A_1 : A_2 : \dots : A_m) \\ &= \sum_{i=1}^m I(A_i : A_1 \dots A_{i-1} A_{i+1} \dots A_m), \end{aligned} \quad (15)$$

i.e. they add up to the sum of all bipartite mutual information between a single system and the rest. In the case of bipartite systems, both candidates are equal to the bipartite mutual information.

In the following section we will show that both mutual information formulas can be used to construct a good entanglement monotone.

Before we define the entanglement measure, let us discuss the problem of conditioning. In general, we do not know what it means to condition upon a quantum register. However it turns out that if a function is a linear combination of entropies, one can condition such a function using a mysterious prescription for conditioning entropy:

$$S(A|B) = S(AB) - S(B).$$

This quantity can be negative, however it has a good interpretation [17]. For linear combination of entropies, we apply this formula to each term. Such conditioning is well defined, in a sense that the result of conditioning does not depend on how we have represented the function in terms of entropies, e.g. a function $f(AB) = S(A) + S(AB) - 2S(AB)$ has the same conditioned version as in the case it is written as $f(AB) = S(A) - S(AB)$. This way of conditioning is rather blind, and it does not tell us how to do it in the case of other functions.

Note that this conditioning reduces to the usual one when the register E is classical. Another interesting feature is the following

$$f(A_1, \dots, A_m | EE') = f((A_1, \dots, A_m | E) | E'), \quad (16)$$

for f a linear combination of entropies and the right hand side has the following meaning: we first compute the function $f(A_1, \dots, A_m | E)$. It is again linear combination of entropies, so one can apply to it conditioning again. Thus conditioning is *associative*.

Since conditioning does not depend on how we decompose the function into entropies, we get that the conditional mutual information is a sum of conditional bipartite mutual information. For example we have:

$$\begin{aligned} I(A_1 : A_2 : \dots | E) &= I(A_1 : A_2 | E) + I(A_3 : A_1 A_2 | E) \\ &\quad + \dots + I(A_m : A_1 \dots A_{m-1} | E). \end{aligned} \quad (17)$$

Let us examine properties of both mutual and conditional mutual information in the multipartite case. We will provide here two properties that were proved in [2] for the bipartite case. It would be very convenient to have a chain rule, however, we do not have it. In place of the chain rule we have two identities that still prove useful:

Proposition 1 *The following identities hold for multipartite*

mutual informations.

$$I(XA_1 : \dots : A_m) = I(A_1 : \dots : A_m|X) + \sum_{i=2}^m I(X : A_i), \quad (18)$$

$$I(XA_1 : \dots : A_m) = I(A_1 : \dots : A_m) + \sum_{i=2}^m I(X : A_i|A_1 \dots A_{i-1}), \quad (19)$$

$$S_m(XA_1 : \dots : A_m) = S_m(A_1 : \dots : A_m|X) + I(X : A_2 \dots A_m), \quad (20)$$

$$S_m(XA_1 : \dots : A_m) = -I(A_2 : \dots : A_m) + \sum_{i=2}^m I(A_i : XA_1 \dots A_{i-1}A_{i+1} \dots A_m). \quad (21)$$

Moreover conditional mutual informations are additive.

Proof. To get identities for I one uses repeatedly the chain rule for bipartite mutual information that asserts $I(XY : Z) = I(X : Z) + I(Y : Z|X)$, and Eq.(11) and Eq.(17). Eq. (20) follows directly from definition (13). The last identity (see [5]) follows from Eqs. (12) and (15).

Additivity follows from the fact that conditional mutual informations are linear combinations of entropies which are additive.

We now immediately get basic monotonicity properties of mutual information (both I and S_m), which are enough to ensure that “squashing” will produce a function that will be a monotone under LOCC.

Proposition 2 *The following statements hold.*

- (i) *Mutual informations do not increase under local conditioning,*

$$I(XA_1 : \dots : A_m) \geq I(A_1 : \dots : A_m|X), \\ S_m(XA_1 : \dots : A_m) \geq S_m(A_1 : \dots : A_m|X). \quad (22)$$

- (ii) *Conditional mutual informations do not increase under local operations,*

$$I(A_1 : \dots : A_m|E) \geq I(\Lambda(A_1) : \dots : A_m|E), \\ S_m(A_1 : \dots : A_m|E) \geq S_m(\Lambda(A_1) : \dots : A_m|E), \quad (23)$$

where $\Lambda(\cdot)$ is a local operation on subsystem A_1 (a trace-preserving completely positive map).

Proof. The statement (i) follows from Eqs.(18) (20), and the fact that bipartite mutual information is nonnegative. The statement (ii) comes from two facts: one is that any local operation can be realized in the unitary representation $\Lambda^Q(\rho_Q) = \text{tr}_R U_{RQ}(|0\rangle\langle 0|)_R \otimes \rho_Q U_{RQ}^\dagger$ and $I(\cdot|E)$ is invariant under local unitary operation and adding ancilla; the other fact is that

$$I(XA_1 : \dots : A_m|E) \geq I(A_1 : \dots : A_m|E). \quad (24)$$

To get Eq.(24), we apply conditioning to both sides of Eq.(19) and using associativity of conditioning obtain

$$I(XA_1 : \dots : A_m|E) = I(A_1 : \dots : A_m|E) + \sum_{i=2}^m I(X : A_i|A_1 \dots A_{i-1}E). \quad (25)$$

Then, the required inequality follows from the fact that bipartite conditional mutual information is nonnegative. Just by conditioning (21) we get the statement (ii) for S_m . This completes the proof. ■

IV. MULTIPARTITE SQUASHED ENTANGLEMENT

In this section we will define two squashed measures and prove that they are monotones under LOCC. One is the q-squashed entanglement when the extension register is quantum. The other is the c-squashed entanglement when the extension register is classical.

A. Monotonicity of entanglement measures under LOCC

First we review what is meant by a monotone under LOCC.

Definition 2 *A function E is called a LOCC monotone if it satisfies the following condition:*

$$E(\rho_{AB}) \geq \sum_i p_i E(\sigma_{AB}^i), \quad (26)$$

where i are outcomes of the LOCC operation, p_i are probabilities of outcomes, and σ_{AB}^i is the state given that outcome i was obtained.

We have the following proposition [18].

Proposition 3 *A convex function f does not increase under LOCC if and only if*

[LUI] *f satisfies local unitary invariance*

$$f(U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger) = f(\rho_{AB}), \quad (27)$$

[FLAGS] *f satisfies*

$$f\left(\sum_i p_i \rho_{AB}^i \otimes |i\rangle_X \langle i|\right) = \sum_i p_i f(\rho_{AB}^i), \quad (28)$$

for $X = A', B'$ where $|i\rangle$ are local, orthogonal “flags”.

B. Q-squashed entanglement

Now we define the multipartite q-squashed entanglement as follows

Definition 3 *For the m party state ρ_{A_1, \dots, A_m}*

$$E_{sq}^q(\rho_{A_1, \dots, A_m}) = \inf I(A_1 : A_2 : \dots : A_m|E), \quad (29)$$

where the infimum is taken over states $\sigma_{A_1, \dots, A_m, E}$ that are extensions of ρ_{A_1, \dots, A_m} , i.e. $\text{Tr}_E \sigma = \rho$.

Alternatively, one can use S_m . We will perform all proofs for I , however we will use only Proposition 2, as well as the fact that if the register E is classical, then conditioning upon it regains its usual meaning. Thus all results are valid also for S_m , so that it gives rise to an independent definition of multipartite squashed entanglement.

The measures we propose reduce to twice the original squashed entanglement in the case of two parties. It resembles

in some respect relative entropy distance from the set of completely separable states, i.e. states of the form

$$\sum_i p_i \rho_{A_1}^i \otimes \dots \otimes \rho_{A_m}^i. \quad (30)$$

Namely, it attributes nonzero entanglement to states that do not contain true multipartite entanglement, such as many singlet pairs. It is immediate to show that E_{sq}^q satisfies condition LUI. In the following we will show that it is convex, and satisfies FLAGS.

Convexity. Consider two states $\rho_{A_1 \dots A_m}$ and $\sigma_{A_1 \dots A_m}$, and their arbitrary extensions $\rho_{A_1 \dots A_m E}$ and $\sigma_{A_1 \dots A_m E}$. We have

$$E_{sq}^q(p\rho_{A_1 \dots A_m} + (1-p)\sigma_{A_1 \dots A_m}) \leq I(A_1 \dots A_m | EE')_\tau \quad (31)$$

with

$$\begin{aligned} \tau_{A_1 \dots A_m EE'} &= p\rho_{A_1 \dots A_m E} \otimes |0\rangle_{E'} \langle 0| \\ &+ (1-p)\sigma_{A_1 \dots A_m E} \otimes |1\rangle_{E'} \langle 1|. \end{aligned} \quad (32)$$

This is because the latter state is an extension of the state $p\rho + (1-p)\sigma$. However, since register E' is classical, the conditioning is reduced to the usual one, so that we have

$$\begin{aligned} I(A_1 \dots A_m | EE')_\tau &= pI(A_1 \dots A_m | E)_\rho \\ &+ (1-p)I(A_1 \dots A_m | E)_\sigma, \end{aligned} \quad (33)$$

where we have used associativity of conditioning. Since we can choose arbitrary extensions of ρ and σ , we get that right-hand-side can be arbitrary close to $pE_{sq}^q(\rho) + (1-p)E_{sq}^q(\sigma)$. This proves convexity. ■

FLAGS. We decompose the condition into two inequalities. The inequality

$$E_{sq}^q\left(\sum_i p_i \rho_{A_1 \dots A_m}^i \otimes |i\rangle_X \langle i|\right) \leq \sum_i p_i E_{sq}^q(\rho_{A_1 \dots A_m}^i) \quad (34)$$

follows from convexity (which we have just proved) and from invariance of E_{sq}^q under adding local pure ancilla. The latter is obvious, since any extension of a state $\rho_{A_1 \dots A_m} \otimes |0\rangle_{A'_1} \langle 0|$ is of the form $\rho_{A_1 \dots A_m E} \otimes |0\rangle_{A'_1} \langle 0|$ where $\rho_{A_1 \dots A_m E}$ is extension of $\rho_{A_1 \dots A_m}$. (Then it follows from additivity of entropy.)

The converse inequality

$$E_{sq}^q\left(\sum_i p_i \rho_{A_1 \dots A_m}^i \otimes |i\rangle_X \langle i|\right) \geq \sum_i p_i E_{sq}^q(\rho_{A_1 \dots A_m}^i) \quad (35)$$

can be interpreted as non-increasing upon conditioning under the local classical register. We have

$$E_{sq}^q\left(\sum_i p_i \rho_{A_1 \dots A_m}^i \otimes |i\rangle_X \langle i|\right) = \inf I(XA_1 : \dots : A_m | E)_\tau, \quad (36)$$

where τ is the extension of the state $\sum_i p_i \rho_{A_1 \dots A_m}^i \otimes |i\rangle_X \langle i|$. Now we dephase register X . Since it is a local operation, according to Prop. 2 the conditional mutual information can only go down. Thus we have

$$\begin{aligned} I(XA_1 : \dots : A_m | E)_\tau &\geq I(XA_1 : \dots : A_m | E)_{\tilde{\tau}} \geq \\ &\geq I(A_1 : \dots : A_m | EX)_{\tilde{\tau}} = \sum_i p_i I(A_1 : \dots : A_m | E)_{\tau_i} \\ &\geq \sum_i p_i E_{sq}^q(\rho_{A_1 \dots A_m}^i), \end{aligned} \quad (37)$$

where $\tilde{\tau}$ is the dephased version of τ and τ_i is the dephased version of τ , given $X = i$, which is still a valid extension of our state. The second inequality comes from Prop. 2. The equality comes from the fact that after dephasing the register is classical. ■

From the definition of E_{sq}^q , we can see that no assumption on the classicality of register E is made. So generally the register E is quantum-correlated with system $A_1 \dots A_m$ in the extensions. What about the case when we allow only classical registers in the extensions i.e. the register and the system is classically correlated? Can it still be a monotone under LOCC? The answer is yes. This comes from the result that we know how to condition any function upon classical registers. In fact, we will show that mutual information is just a special case immediately obtained from a general theorem.

Remark: In a recent paper [19], the bipartite squashed entanglement was given an operational interpretation in terms of communication rate in state merging. In [20], the multipartite q-squashed entanglement on I_m with the factor $1/2$ was developed independently and was related to the outer bound on the communication rate in multipartite distributed compression. To find a similar situation for the multipartite q-squashed entanglement on S_m is an open question.

C. Additivity of q-squashed entanglement

In this section we show that the two versions of multipartite q-squashed entanglement are additive on tensor product and subadditive in general. Namely it turns out that the main ideas behind the proof of additivity of bipartite squashed entanglement can be carried over to multipartite case. We will show explicitly the proof for three parties. The generalization of n parties is immediate.

The main ingredient is the following lemma.

Lemma 1

$$\begin{aligned} I(AA' : BB' : CC' | E) &= I(A : B : C | A'B'C'E) \\ &+ I(A' : B' : C' | E) + I(A : B'C' | A'E) \\ &+ I(B : A'C' | B'E) + I(C : A'B' | C'E), \end{aligned} \quad (38)$$

$$\begin{aligned} S_3(AA' : BB' : CC' | E) &= S_3(A : B : C | A'B'C'E) \\ &+ S_3(A' : B' : C' | E) + I(AB : C' | A'B'E) \\ &+ I(AC : B' | A'C'E) + I(BC : A' | B'C'E). \end{aligned} \quad (39)$$

Proof.

$$\begin{aligned} &I(AA' : BB' : CC' | E) - I(A : B : C | A'B'C'E) \\ &\quad - I(A' : B' : C' | E) \\ &= S(AA'E) + S(BB'E) + S(CC'E) \\ &\quad + 3S(A'B'C'E) - S(AA'B'C'E) - S(BA'B'C'E) \\ &\quad - S(CA'B'C'E) - S(A'E) - S(B'E) - S(C'E) \\ &= S(AA'E) + S(A'B'C'E) - S(AA'B'C'E) \\ &\quad - S(A'E) + S(BB'E) + S(A'B'C'E) \\ &\quad - S(BA'B'C'E) - S(B'E) + S(CC'E) \\ &\quad + S(A'B'C'E) - S(CA'B'C'E) - S(C'E). \end{aligned} \quad (40)$$

$$\begin{aligned}
& S_3(AA' : BB' : CC' | E) - S_3(A : B : C | A'B'C'E) \\
& \quad - S_3(A' : B' : C' | E) \\
& = S(AA'BB'E) + S(AA'CC'E) + S(BB'CC'E) \\
& \quad - S(ABA'B'C'E) \\
& \quad - S(ACA'B'C'E) - S(BCA'B'C'E) + 3S(A'B'C'E) \\
& \quad - S(A'B'E) - S(A'C'E) - S(B'C'E) \\
& = I(AB : C' | A'B'E) + I(BC : A' | B'C'E) \\
& \quad + I(CA : B' | C'A'E). \blacksquare \quad (41)
\end{aligned}$$

Since conditional mutual information is positive, we obtain immediately

Corollary 1

$$I(AA' : BB' : CC' | E) \geq I(A : B : C | A'B'C'E) + I(A' : B' : C' | E), \quad (42)$$

$$S_3(AA' : BB' : CC' | E) \geq S_3(A : B : C | A'B'C'E) + S_3(A' : B' : C' | E). \quad (43)$$

The lemma 1 allows also to prove:

Lemma 2 Conditional I and S_3 are additive. For product states $\rho_{ABCE} \otimes \sigma_{A'B'C'E'}$

$$I(AA' : BB' : CC' | EE') = I(A : B : C | E) + I(A' : B' : C' | E'), \quad (44)$$

$$S_3(AA' : BB' : CC' | EE') = S_3(A : B : C | E) + S_3(A' : B' : C' | E'). \quad (45)$$

Proof. From lemma 1 we get

$$\begin{aligned}
I(AA' : BB' : CC' | EE') & = I(A : B : C | A'B'C'EE') \\
& \quad + I(A' : B' : C' | EE') + \underbrace{I(A : B'C' | A'EE')}_{=0} \\
& \quad + \underbrace{I(B : A'C' | B'EE')}_{=0} + \underbrace{I(C : A'B' | C'EE')}_{=0}, \\
& = I(A : B : C | E) + I(A' : B' : C' | E'). \quad (46)
\end{aligned}$$

The last three terms vanish because the state is a tensor product: the primed systems are not correlated with the non-primed. Similarly:

$$\begin{aligned}
S_3(AA' : BB' : CC' | EE') & = S_3(A : B : C | A'B'C'EE') \\
& \quad + S_3(A' : B' : C' | EE') + \underbrace{I(AB : C' | A'B'EE')}_{=0} \\
& \quad + \underbrace{I(AC : B' | A'C'EE')}_{=0} + \underbrace{I(BC : A' | B'C'EE')}_{=0} \\
& = S_3(A : B : C | E) + S_3(A' : B' : C' | E'), \quad (47)
\end{aligned}$$

which ends the proof. An immediate conclusion from the corollary 1 and lemma 2 is that E_{sq}^q based on either of the mutual informations is additive.

Proposition 4 For any n -partite states ρ and σ ,

$$E_{sq}^q(\rho \otimes \sigma) = E_{sq}^q(\rho) + E_{sq}^q(\sigma). \quad (48)$$

From Corollary 1 it follows that E_{sq}^q is superadditive,

$$E_{sq}^q(\rho_{12}) \geq E_{sq}^q(\rho_1) + E_{sq}^q(\rho_2), \quad (49)$$

where the subscripts denote two n partite systems.

D. Entanglement measures via mixed convex roof

In this subsection, we prove a theorem that provides a method of constructing entanglement measures via mixed convex roof.

Definition 4 A mixed convex roof of a function g is given by

$$E_g(\rho) = \inf \sum_i p_i g(\rho_i), \quad (50)$$

where infimum is taken over all ensembles $\{p_i, \rho_i\}$ satisfying $\sum_i p_i \rho_i = \rho$.

Remark: In [8] it was shown that if g is continuous, then there exists a finite decomposition that realizes the infimum. Moreover it was shown, that if g is asymptotically continuous, then so is its mixed convex roof (which is a generalization of [21]).

Theorem 1 For any continuous function g which is a monotone on average under local operations, its mixed convex roof is monotonic under LOCC.

Let us recall that to prove monotonicity of multipartite squashed entanglement we have used two features of mutual information proven in proposition 2: monotonicity under local operations, and monotonicity under local conditioning. Note that those two features, if we consider only conditioning upon classical register, are equivalent to monotonicity on average under local operations.

Proof. First, it is immediate to see that E_g is convex. It remains to show that also E_g is monotone under local measurements, on average [22]. We will simply show that for any given measurement, if g does not increase under this measurement for any state, E_g does not either. Consider arbitrary state ρ with optimal decomposition $\{p_i, \rho_i\}$ (if there does not exist such ensemble, we can take a nearly optimal one, and the proof still goes through). The measurement transforms the state ρ into ensemble:

$$\rho \rightarrow \{q_k, \sigma_k\} \quad (51)$$

and the members ρ_i of the optimal ensemble into ensembles $\{q_{k|i}, \sigma_k^{(i)}\}$. Thus $q_{k|i}$ is the probability of obtaining outcome k provided the state ρ_i was sent. The probability that ρ_i was sent, if outcome k was obtained is given by $q_{i|k} = p_i q_{k|i} / q_k$. Note that

$$\sum_i q_{i|k} \sigma_k^{(i)} = \sigma_k. \quad (52)$$

Now we have

$$\begin{aligned}
E_g(\rho) & = \sum_i p_i g(\rho_i) \geq \sum_i p_i \sum_k q_{k|i} g(\sigma_k^{(i)}) \\
& = \sum_k q_k \sum_i q_{i|k} g(\sigma_k^{(i)}) \geq \sum_k q_k E_g(\sigma_k). \quad (53)
\end{aligned}$$

The first equality comes from the fact that the ensemble $\{p_i, \rho_i\}$ is optimal, whose existence is guaranteed by continuity of g (see above remark). The first inequality comes from monotonicity of g under the considered measurement. The last inequality, comes from the fact that $\{q_{i|k}, \sigma_k^{(i)}\}$ is some ensemble of σ_k (it follows from Eq.(52)). This completes the proof. ■

A new entanglement measure can be constructed via mixed convex roof if a function satisfying the condition of the theorem is found. An example illustrating the theorem is that one can take as g the function I_c , defined as supremum of mutual information of the joint probability distribution after Bob and Alice's measurement. That is

$$I_c(\rho_{AB}) = \sup_{A_i^\dagger A_i, B_i^\dagger B_i} H(p_A) + H(p_B) - H(p_{AB}), \quad (54)$$

where $p_{AB}^i = \text{tr} A_i \otimes B_i \rho_{AB} A_i^\dagger \otimes B_i^\dagger$. Another one is the c-squashed entanglement defined below.

E. C-squashed entanglement

Multipartite c-squashed entanglement is defined as follows.

Definition 5 For the m party state ρ_{A_1, \dots, A_m}

$$E_{sq}^c(\rho_{A_1, \dots, A_m}) = \inf I(A_1 : A_2 : \dots : A_m | E), \quad (55)$$

where infimum is taken over the extension states $\sigma_{A_1, \dots, A_m, E}$ of the form $\sum p_i \rho_{A_1 \dots A_m}^i \otimes |i\rangle_E \langle i|$.

It is clear that E_{sq}^c is nothing but the entanglement measure obtained by mixed convex roof of multipartite quantum mutual information function. We have seen that multipartite quantum mutual information satisfies the conditions of the theorem. This function was considered in [7] in the context of distillation of private key. Its bipartite version was also presented in [1], [10]. By the theorem, we get that it is indeed a good entanglement measure. The measure is related to the q-squashed entanglement: it is obtained, if in the definition of "squashing", one restricts to extensions such that the auxiliary system is classical.

Of course by replacing I with S_m we obtain another version of c-squashed entanglement. In bipartite case, it coincides with the previous one.

F. Asymptotic continuity

In this subsection, we prove the asymptotic continuity of E_{sq}^q and E_{sq}^c .

Definition 6 Let f be a real-valued function f defined on states ρ_1, ρ_2 acting on Hilbert space C^d and $\epsilon = \|\rho_1 - \rho_2\|_1$. Then a function is asymptotically continuous if it fulfils the following condition

$$\forall \rho_1, \rho_2 |f(\rho_1) - f(\rho_2)| \leq K_1 \epsilon \log d + O(\epsilon), \quad (56)$$

where K_1 is constant and $O(\epsilon)$ is any function, which satisfies $\lim_{\epsilon \rightarrow 0} O(\epsilon) \rightarrow 0$ and depends only on ϵ . (In particular, it does not depend on the dimension).

Proposition 5 The multipartite q -squashed entanglement $E_{sq}^q(A_1 \dots A_m)$ and c -squashed entanglement $E_{sq}^c(A_1 \dots A_m)$ are asymptotically continuous.

Proof. The asymptotic continuity of $E_{sq}^q(A_1 \dots A_m)$ comes from Eq.(17) and Alicki-Fannes result [11] that asserts $I(A : B | E)$ is asymptotically continuous and $d = d_A$. The asymptotic continuity of $E_{sq}^c(A_1 \dots A_m)$ comes from the fact that the mixed convex roof of a function inherit the asymptotic continuity of that function [8].

G. Lockability property

In this subsection, we will calculate squashed entanglement for the multipartite flower state and show that multipartite squashed entanglement is lockable. A quantity, usually some measure of correlations, is lockable if it can drop by an arbitrary amount when only a single qubit of a local system is lost. This property has previously been observed for many correlation measures such as accessible information, entanglement cost and logarithmic negativity [23], [24], [25]. The bipartite squashed entanglement has been proved to be lockable in [26]. Here we adapt the proof to the multipartite case. First we generalize the flower state to multipartite case.

Definition 7 A tripartite flower state $\rho_{AA'BB'CC'}$ is defined through its purification state $|\Phi\rangle_{AA'BB'CC'X}$ of the form,

$$|\Phi\rangle_{AA'BB'CC'X} = \frac{1}{\sqrt{2d}} \sum_{i=1, \dots, d} |i\rangle_A |j\rangle_{A'} |i\rangle_B |j\rangle_{B'} |i\rangle_C |j\rangle_{C'} U_j |i\rangle_X, \quad (57)$$

where $U_0 = I$ and U_1 is a Fourier transform.

Proposition 6 For the tripartite flower state, $E_{sq}^q(AA' : BB' : CC') = 3 + \log d$, $E_{sq}^c(AA' : BB' : CC') = 3 + \frac{3}{2} \log d$ for the version I_3 and $E_{sq}^q(AA' : BB' : CC') = E_{sq}^c(AA' : BB' : CC') = 3 + \log d$ for S_3 while $E_{sq}^{(c)}(A : BB' : CC') = 0$ for both I_3 and S_3 .

Proof. The minimization over state extensions $\rho_{AA'BB'CC'Z}$ in squashed entanglement is equivalent to a minimization over CPTP channels $\Lambda : X \rightarrow Z$, acting on the purifying system X for $\rho_{AA'BB'CC'}$,

$$\rho_{AA'BB'CC'Z} = (id_{AA'BB'CC'} \otimes \Lambda) \Phi_{AA'BB'CC'X}. \quad (58)$$

Now we use the result proved in [26] that asserts for the bipartite flower state $\sigma_{AA'BB'}$:

$$S(AA'Z) + S(BB'Z) - S(AA'BB'Z) - S(Z) \geq 2 + \log d, \quad (59)$$

where the equality can be reached by trivial Z (i.e. Z is product with the rest) or by $Z = X$, or finally, by measuring Z in basis $\{|i\rangle\}$.

For the q-squashed I_3 ,

$$I(AA' : BB' : CC' | Z) = AA'Z + BB'Z + CC'Z - AA'BB'CC'Z - 2Z$$

$$= \frac{1}{2} \underbrace{[AA'Z + BB'Z - AA'BB'CC'Z - Z]}_{\geq 2+\log d} \quad (60)$$

$$+ \frac{1}{2} \underbrace{[BB'Z + CC'Z - AA'BB'CC'Z - Z]}_{\geq 2+\log d} \quad (61)$$

$$+ \frac{1}{2} \underbrace{[CC'Z + AA'Z - AA'BB'CC'Z - Z]}_{\geq 2+\log d} \quad (62)$$

$$+ \frac{1}{2} \underbrace{[AA'BB'CC'Z - Z]}_{\geq -S(AA'BB'CC') = -\log d} \quad (63)$$

$$\geq 3 + \log d, \quad (64)$$

where we omitted $S()$ for brevity. Ineqs. (60),(61) and (62) come from Ineq.(59) and the facts that $S_\rho(AA'Z) = S_\rho(BB'Z) = S_\rho(CC'Z) = S_\sigma(AA'Z) = S_\sigma(BB'Z)$ and $S_\rho(AA'BB'CC'Z) = S_\sigma(AA'BB'Z)$, Ineq.(63) from the subadditivity of von Neumann entropy. It is easy to check that $I(AA' : BB' : CC'|Z) = 3 + \log d$ if the extension state is the purification one.

If the register is classical, then $\rho_{AA'BB'CC'Z}$ is necessarily separable in $AA'BB'CC' : Z$. Therefore Ineq.(63) should be replaced by $[S(AA'BB'CC'Z) - S(Z)] \geq 0$. On the other hand, if $\rho_{AA'BB'CC'Z}$ is the state after the measurement on X in the basis $\{|1\rangle, \dots, |d\rangle\}$, then the bound is achieved. So $E_{sq}^c = 3 + \frac{3}{2} \log d$.

For the q-squashed S_3 ,

$$\begin{aligned} S(AA' : BB' : CC'|Z) &= AA'BB'Z + BB'CC'Z \\ &\quad + CC'AA'Z - 2AA'BB'CC'Z - Z \\ &= \frac{1}{2} \underbrace{[AA'BB'Z + BB'CC'Z - AA'BB'CC'Z - Z]}_{\geq 2+\log d} \quad (65) \end{aligned}$$

$$+ \frac{1}{2} \underbrace{[BB'CC'Z + CC'AA'Z - AA'BB'CC'Z - Z]}_{\geq 2+\log d} \quad (66)$$

$$+ \frac{1}{2} \underbrace{[CC'AA'Z + AA'BB'Z - AA'BB'CC'Z - Z]}_{\geq 2+\log d} \quad (67)$$

$$\begin{aligned} &+ \frac{1}{2} \underbrace{[Z - AA'BB'CC'Z]}_{\geq -S(AA'BB'CC') = -\log d} \quad (68) \\ &\geq 3 + \log d, \quad (69) \end{aligned}$$

where again we omit $S()$ for brevity. The above inequalities hold for similar reasons. One also can check that $S(AA' : BB' : CC'|Z) = 3 + \log d$ if the extension of the state is trivial (i.e. the state itself tensored with some state of Z) that also means the c-squashed entanglement is equal to the q-squashed one.

On the other hand, $\rho_{ABB'CC'}$ is separable, so $E_{sq}^{q(c)}(\rho_{ABB'CC'}) = 0$ for both versions. This shows that the multipartite squashed entanglement is lockable. ■

The results can be straightforwardly generalized to the m -partite flower state. In particular for I_m , we have $E_{sq}^q = m + \log d$, and $E_{sq}^c = m + \frac{m}{2} \log d$, while for S_m we have $E_{sq}^q = E_{sq}^c = m + \log d$.

Remark: It is notable that during the proof, the q-squashed entanglement of flower state is achieved by the purifying register for I_3 that is necessarily quantum (the equality in Ineq.(63) holds only if $AA'BB'CC'Z$ is in a pure state), while by trivial extension for S_3 that can be classical. Moreover the c-squashed entanglement can be arbitrarily larger than the q-squashed one. This gives the negative answer to the open question: “Is q-squashed entanglement equal to c-squashed entanglement for the version of I_m ?” for the multipartite case. For the bipartite case, we cannot see it from the flower state. Note that quite recently Brandao [27] has proved that E_{sq}^c and E_{sq}^q are different even in bipartite case, for antisymmetric Werner states. Now, one can also ask, whether the two versions of squashed entanglement, coming from S_m and I_m respectively, are different from each other. For pure states and the flower states, we see that q-squashed entanglement is equal for two versions. Are these two versions the same in the end? We don't know now. But as we have shown, for c-squashed entanglement the two versions *are* different. We then guess, that also for q-squashed entanglement they are different.

V. MULTIPARTITE AXIOMATIC MONOTONES AS AN UPPER BOUND ON DISTILLABLE KEY

In this section we will show, that the quantum squashed entanglement is an upper bound on multipartite distillable key [13]. We will do this by proving that a wide class of entanglement monotones, which satisfy some natural axioms are upper bounds on distillable key. That is we generalize the results of [12] (see also [28]) to a multipartite case. We also revisit the analogous result within the so called classical key agreement framework [29] (see also [30], [31]), that has been given in [5]. There, an even a more general approach has been developed: the rates of transition between the probability distributions under LOPC operations are considered, and the classical multipartite secrecy monotones are shown to govern these rates. In section V-D we show again that the classical secrecy monotones are upper bounds on classical distillable key, addressing more carefully the issue of asymptotic continuity and consider more explicitly the presence of the eavesdropper.

In what follows, we will use a short-hand notation for multipartite systems. In particular $\tilde{A}_1 \dots \tilde{A}_m$ we denote as $(m)\tilde{A}$. We will assume that $\tilde{A}_i = A_i A'_i$ and sometimes we denote $(m)\tilde{A}$ more explicitly as $(m)AA'$. We denote also $A_1 \dots A_m$ as $(m)A$ and $A'_1 \dots A'_m$ as $(m)A'$. Following this rule, the Hilbert space $\mathcal{H}_{\tilde{A}_1} \otimes \dots \otimes \mathcal{H}_{\tilde{A}_m}$ will be denoted as $\mathcal{H}_{(m)\tilde{A}}$, and $\mathcal{H}_{\tilde{A}_1}^{(n)} \otimes \dots \otimes \mathcal{H}_{\tilde{A}_m}^{(n)}$ which is isomorphic with the tensor product of n copies of $\mathcal{H}_{(m)\tilde{A}}$, as $\mathcal{H}_{(m)\tilde{A}}^{(n)}$. Consequently, the state ρ of such system will be denoted as $\rho_{(m)\tilde{A}}$. Analogously we mean $\rho_{(m)A'}$ as acting on $B(\mathcal{H}_{(m)A'}) = B(\mathcal{H}_{A'_1} \otimes \dots \otimes \mathcal{H}_{A'_m})$ and $\rho_{(m)A}$ as the state acting on $B(\mathcal{H}_{(m)A}) = B(\mathcal{H}_{A_1} \otimes \dots \otimes \mathcal{H}_{A_m})$.

A. Multipartite key distillation

Let us first recall the definition of multipartite distillable key in the context of private quantum states [32]. It was introduced in [32] and is studied in [13], as a direct generalization of the

bipartite case. Namely, instead of twisted maximally entangled bipartite states, the parties have to distill a twisted GHZ state, so that m -partite private dit has a form:

$$\gamma_m^{(d)} = \sum_{i,j=0}^{d-1} \frac{1}{d} |i\dots i\rangle\langle j\dots j| \otimes U_i \rho_{A'_1, \dots, A'_m} U_j^\dagger, \quad (70)$$

where U_i are some unitary operations acting on $\mathcal{H}_{A'_1, \dots, A'_m}$.

The optimal rate of key $\frac{\log d}{n}$ distilled by means of LOCC operations from n copies of the input state is the multipartite distillable key, which is denoted as $K_D^{(m)}$. Let us note here, that in what follows, for technical reasons we will denote by m the number of parties of a multipartite state and by n the number of copies of the state. More formally, we have:

Definition 8 For any given state $\rho_{(m)\tilde{A}} \in \mathcal{B}(\mathcal{H}_{(m)\tilde{A}})$ let us consider a sequence P_n of LOCC operations such that $P_n(\rho_{(m)\tilde{A}}^{\otimes n}) = \sigma_n$. A set of operations $\mathcal{P} \equiv \cup_{n=1}^{\infty} \{P_n\}$ is called a pdit distillation protocol of state $\rho_{(m)\tilde{A}}$ if there holds

$$\lim_{n \rightarrow \infty} \|\sigma_n - \gamma_m^{d_n}\| = 0, \quad (71)$$

where γ_{d_n} is a multipartite pdit whose key part is of dimension $d_n \times d_n$.

For a protocol \mathcal{P} , its rate is given by

$$\mathcal{R}(\mathcal{P}) = \limsup_{n \rightarrow \infty} \frac{\log d_n}{n}. \quad (72)$$

The distillable key of state $\rho_{(m)\tilde{A}}$ is given by

$$K_D^{(m)}(\rho_{(m)\tilde{A}}) = \sup_{\mathcal{P}} \mathcal{R}(\mathcal{P}). \quad (73)$$

Remark 1 In Sec. V-C we will show that the maximization in the definition of $K_D^{(m)}$ can be restricted to protocols whose communication complexity grows at most linearly in the number of copies of the initial state $\rho_{(m)\tilde{A}E}$ (lemma 3). Moreover, the optimal yield can be obtained with the use of a number of systems (needed for implementing local operations), that grows also linearly in the number of the input copies (remark 2). Hence, if $d = \dim \mathcal{H}_{(m)\tilde{A}E} < \infty$ then the dimension of the output of the protocol is bounded by $\log \dim \mathcal{H}_{(m)\tilde{A}E} \leq cn \log d$, for some constant c .

B. Upper bounds from monotonicity

Following the paper by Ekert et al. [12], we know that a function is an upper bound on distillable key C_D , if it satisfies some natural axioms. Their proof can be generalized to the multipartite case, as it does not depend on the number of parties. Actually, the only fact which is needed here is that there is a protocol P with the property that on the n copies of the m -partite state $\rho_{(m)\tilde{A}}$, satisfying

$$\|\rho_{(m)\tilde{A}} - \gamma_m^{(d)}\| \leq \epsilon \quad (74)$$

that uses only linear communication (in the number of copies of ρ) and has a rate close to $\log d$ (i.e. $\log d - f(\epsilon)$ with f vanishing as ϵ approaches zero). More formally it is stated in

the theorem below a multipartite version of the Corollary 3.2. from [12].

Theorem 2 Let $M(\rho)$ be a function mapping (m) -partite quantum states $\rho \equiv \rho_{(m)AA'}$ into the positive numbers such that the following holds:

- 1) *Monotonicity:* $M(\Lambda(\rho)) \leq M(\rho)$ for any LOCC operation Λ .
- 2) *Asymptotic continuity:* for any states ρ^n, σ^n acting on $\mathcal{H}_{(m)\tilde{A}}^{(n)}$, the condition $\|\rho^n - \sigma^n\| \rightarrow 0$ implies $\frac{1}{\log r_n} |M(\rho^n) - M(\sigma^n)| \rightarrow 0$ where $r_n = \dim \mathcal{H}_{(m)\tilde{A}}^{(n)}$.
- 3) *Normalisation:* $M(\gamma^{(\ell)}) \geq \ell$.

Then the regularisation of the function M given by $M^\infty(\rho) = \limsup_{n \rightarrow \infty} \frac{M(\rho^{\otimes n})}{n}$ is an upper bound on $K_D^{(m)}$, i.e., $M^\infty(\rho_{(m)AA'}) \geq K_D^{(m)}(\rho_{(m)AA'})$ for all $\rho_{(m)AA'}$ with $\dim \mathcal{H}_{(m)\tilde{A}}^{(n)} < \infty$. If in addition M satisfies

4. *Subadditivity on tensor products:* $M(\rho^{\otimes n}) \leq nM(\rho)$, then M is an upper bound for $K_D^{(m)}$.

Proof. This theorem follows as a corollary from the multipartite version of the theorem 3.1. of [12]. Since the proof of the multipartite version does not differ from the one for the tripartite case, we refer the reader to [12]. We note however, that the latter proof uses the fact stated in lemma A.1. of [12]. We provide in section V-C an analogous lemma in the multipartite case - which proves the first statement of our remark 1. We show there that the amount of classical communication needed by an optimal key distillation protocol is linear in the number of systems n .

We note here also that the proof given in [12] based implicitly on the fact that only communication can increase the dimension of the support of the output state of an optimal key distillation protocol. Although this fact does hold, as it can be proved directly using quantum information techniques, we provide shorter argumentation in Remark 2. ■

Example 1 (multipartite squashed entanglement as an upper bound on distillable key)

As an example of the application of theorem 2, we show here that the normalized multipartite squashed entanglement is an upper bound on the distillable key:

$$\frac{1}{m} E_{sq}^q(\rho) \geq K_D^{(m)}(\rho). \quad (75)$$

To see this we observe that this monotone easily fulfils the conditions (1), (2) and (4) of theorem 2, as is shown in sections IV-B, IV-F and IV-C respectively. What remains to check the normalization condition which we show in the observation below.

Observation 1 For any natural $m \geq 2$ there holds: $E_{sq}^q(\gamma_m^{(d)}) \geq m \log d$.

Proof. The proof is just a direct generalization of that given in [28] for the bipartite case ($m = 2$). In what follows we fix a natural $m \geq 3$ arbitrarily.

We consider a state $\rho_{(m)AA'} = |\Psi_+^{(d)}\rangle \otimes \rho_{(m)A'}$ and its extension to system E $\rho_{(m)AA'E} \equiv \rho$. We have also

$\gamma \equiv \gamma_{(m)AA'E}^{(d)} = U \otimes \mathbb{I}_E(\rho_{(m)AA'E})U^\dagger \otimes \mathbb{I}_E$, where $U = \sum_{i=0}^{d-1} |i \dots i\rangle\langle i \dots i| \otimes U_i^{(m)A'}$ is a twisting operation.

We then have the following facts:

1)

$$\begin{aligned} S((m)AA'E)_\gamma &= S((m)AA'E)_\rho \\ &= S((m)A'E)_\rho = S((m)A'E)_{\gamma_i}, \end{aligned} \quad (76)$$

where $\gamma_i^{(m)A'E} = U_i^{(m)A'} \otimes \mathbb{I}_E(\rho_{(m)A'E})[U_i^{(m)A'}]^\dagger \otimes \mathbb{I}_E$.

2) $S(E)_{\gamma_i} = S(E)_\gamma$, where γ_i^E ($\gamma_i^{(m)A'E}$) denotes the E subsystem of $\gamma_{(m)AA'E}$ ($\gamma_i^{(m)A'E}$).

3)

$$\forall_{i \in 1, \dots, m} S(A_i A'_i E)_\gamma = \log d + \sum_{k=0}^{d-1} \frac{1}{d} S(A'_i E)_{\gamma_k}. \quad (77)$$

The first fact is obvious due to unitarity relations between $\rho_{(m)AA'E}$ and $\gamma_{(m)AA'E}$, as well as $\rho_{(m)A'}$ and $\gamma_i^{(m)A'}$. The second one is just a consequence of the fact that $\gamma_i^E = \gamma_E$. The third one follows from the fact that the $A_i A'_i E$ subsystem is a *cqq* state and from the joint entropy theorem [33].

Having established these facts, the argumentation is straightforward. Let E be the fixed extension. By definition of the squashed entanglement [1], [2] we have:

$$\begin{aligned} E_{sq}^q(\gamma_m^{(d)}) &= \inf_E I((m)AA'|E)_\gamma \\ &= \inf_E \left[\sum_{i=1}^m S(A_i A'_i E)_\gamma \right. \\ &\quad \left. - (m-1)S(E)_\gamma - S((m)AA'E)_\gamma \right] \end{aligned}$$

$$= m \log d + \inf_E \left[\sum_{i=1}^m \sum_{k=0}^{d-1} \frac{1}{d} S(A'_i E)_{\gamma_k} \right. \\ \left. - (m-1)S(E)_\gamma - S((m)AA'E)_\gamma \right] \quad (78)$$

$$= m \log d + \inf_E \left[\sum_{k=0}^{d-1} \frac{1}{d} \left(\sum_{i=1}^m S(A'_i E)_{\gamma_k} \right) \right. \\ \left. - (m-1)S(E)_{\gamma_k} - S((m)A'E)_{\gamma_k} \right] \quad (79)$$

$$= m \log d + \inf_E \sum_{k=0}^{d-1} \frac{1}{d} I((m)A'|E)_{\gamma_k} \quad (80)$$

$$\geq m \log d. \quad (81)$$

In equality (79) we have used the fact (3) while in (80) the facts (1) and (2). The last inequality is thanks to the positivity of conditional multipartite mutual information. Since the choice of $m \geq 3$ was arbitrary, we have proved the lemma.

C. Linear communication cost of optimal multipartite key distillation

In this section we show, that, as in the bipartite case, an optimal key distillation protocol needs only a linear amount of communication. To this end, we use the following theorem, that is proved in [13]:

Theorem 3 For any state $\rho_{(m)\tilde{A}}$ of the systems $(m)\tilde{A}$ with $\tilde{A}_i = A_i A'_i$, there is a protocol \mathcal{P} with a rate:

$$K_D^{\mathcal{P}}(\rho_{(m)\tilde{A}}) \geq \min_{i \neq 1} I(A_1 : A_i)_{\psi_\rho} - I(A_1 : E)_{\psi_\rho}, \quad (82)$$

where ψ_ρ is a purification of the state $\rho_{(m)\tilde{A}}$ to system E . On n input copies the protocol \mathcal{P} uses cn bits of classical communication, for some constant $c > 0$.

Remark 2 Another property of the protocol given in [13], is that it uses the ancillary systems to implement local operations with dimension that is only linear in the number of input states n . To see this, we just observe that the party which broadcasts to the other parties does not need any ancillary systems, and the remaining $m-1$ parties needs no more of them than the rate of the key, which is clearly linear in n .

We can give now the final lemma which proves the statement from remark 1. This is a modified version of the lemma A.1., given in [12].

Lemma 3 (Comp. lemma A.1. [12]).

The maximization in the definition $K_D^{(m)}$ can be restricted to protocols that use communication at most linear in the number of copies of $\rho_{(m)AA'}$. This implies that if $\dim \mathcal{H}_{(m)\tilde{A}} = d < \infty$ then $\dim \mathcal{H}_{(m)\tilde{A}}^{(n)} \leq cn \log d$, where c is a constant independent of d and n .

Proof. In what follows we directly reproduce a bipartite proof given in [12].

Let $\{\Lambda_n\}_{n \in \mathbb{N}}$ be a key distillation protocol (with communication not necessarily linear in n) with rate R . For any fixed $\epsilon > 0$, there exists an n_0 such that

$$\|\Lambda_{n_0}(\rho_{(m)AA'}^{\otimes n_0}) - \gamma_{(m)A}^{\ell_{n_0}}\|_1 \leq \epsilon, \quad (83)$$

and $\frac{\ell_{n_0}}{n_0} \geq R - \epsilon$. Consider now key distillation from many copies of $\sigma_{(m)AE} := \Delta(\Lambda_{n_0}(\rho_{(m)AA'}^{\otimes n_0}))$, where Δ is a measurement of Alice and Bob in their computational bases followed by tracing out the systems $(m)A'$ (and the same for Bob). Using Fannes' inequality [34] we can bound the difference in the mutual informations by

$$\min_{i \neq 1} I(A_1 : A_i)_{\psi_\sigma} - I(A_1 : E)_{\psi_\sigma} \geq \ell_{n_0} - 4\epsilon \ell_{n_0} - 6\eta(\epsilon), \quad (84)$$

where ψ_σ is a purification of the state σ . As it is assured by theorem 3, Alice and Bob are now able to achieve a rate $\min_{i \neq 1} I(A_1 : A_i)_{\psi_\sigma} - I(A_1 : E)_{\psi_\sigma}$ using communication linear in the number of copies of $\sigma_{(m)A}$. We therefore have modified the protocol $\{\Lambda_n\}_{n \in \mathbb{N}}$ achieving a rate R into a protocol $\{\tilde{\Lambda}_n\}_{n \in \mathbb{N}}$ with a rate

$$\tilde{R} \geq (1 - c\epsilon)(R - \epsilon) - \frac{c'h(\epsilon)}{n_0}. \quad (85)$$

The amount of communication needed is proportional to the number of copies of $\rho_{(m)AA'}$. Since ϵ was arbitrary we obtain a sequence of protocols (with communication linear in the number of copies $\rho_{(m)AA'}$) approaching the rate R . ■

D. Analogous results for multipartite classical key agreement

In this section we will consider the analogous result to the ones given in theorem 2, in the realm of *classical key agreement* [29], [30], [31], that has been found in [5]. Within this paradigm, the distillable key from an $m+1$ -partite

distribution is the amount of key that can be obtained in the asymptotic limit from the n realizations of a distribution via local operations and communication between m parties $(m)A$ which is public i.e. listened to by the $m+1$ -th party - Eve, per copy of a distribution. We will show that a function of an $m+1$ -partite distribution, which satisfies axioms of monotonicity, continuity, normalization and subadditivity, is an upper bound on the amount of secure key that can be distilled from the $m+1$ partite distribution (*distillable key*).

In what follows $P_{(m)A}$ will denote a distribution defined on $\chi_{(m)A} = \chi_{A_1} \times \dots \times \chi_{A_m}$. The n such distributions resides consequently on $\chi_{A_1}^n \times \dots \times \chi_{A_m}^n$, which is denoted as $\chi_{(m)A}^n$. Analogously, $\chi_{A'_1}^n \times \dots \times \chi_{A'_m}^n \times E'$ will be denoted as $\chi_{(m)A'E'}^n$.

For the sake of completeness of the presentation, we begin with definition of an LOPC protocol:

Definition 9 An LOPC protocol \mathcal{P} is an family $\{\Lambda\}_n$ of classical channels $\Lambda_n : (\chi_{(m)AE}^n) \rightarrow \chi_{(m)A'E'}^n$, which are a finite number of concatenation of local operations (local channels) and public communication steps (communicating some number to one honest party and the eavesdropper).

We pass now to definition of distillable secure key, that is the key that can be obtained from a given distribution via an (optimal) LOPC protocol:

Definition 10 We say that LOPC protocol \mathcal{P} is a classical key distillation protocol for a distribution $P_{(m)A} \in \chi_{(m)A}$, if

$$\lim_{n \rightarrow \infty} \|\Lambda_n(P_{(m)A}^{\otimes n}) - K_{(m)A}^{l_n}\| = 0, \quad (86)$$

where $K_{(m)A}^{l_n} = \frac{1}{l_n}(i_1 \dots i_m) \delta_{i_1 \dots i_m} \otimes P_E$ is the ideal key distribution on $\chi_{(m)A}$, for some distribution P_E of the eavesdropper. The rate of a protocol is given by

$$\mathcal{R}(\mathcal{P}) = \limsup_{n \rightarrow \infty} \frac{\log l_n}{n}. \quad (87)$$

Then the classical distillable key of a distribution $P_{(m)A}$ is defined as supremum of the rates

$$C_D^{(m)}(P_{(m)A}) = \sup_{\mathcal{P}} \mathcal{R}(\mathcal{P}). \quad (88)$$

Consequently, we have the following theorem:

Theorem 4 (See also a general result of [5]) Let M be a function mapping $m+1$ -partite classical distributions (defined on $\chi_m^n = \chi_{A_1}^n \times \dots \times \chi_{A_m}^n \times \chi_E^n$) into positive numbers such that there holds:

- 1) Monotonicity: $M(\Lambda(P)) \leq M(P)$ for any LOPC operation Λ .
- 2) Asymptotic continuity: for any distributions P^n, Q^n defined on χ_m^n , the condition $\|P^n - Q^n\| \rightarrow 0$ implies $\frac{1}{\log r_n} |M(P^n) - M(Q^n)| \rightarrow 0$ where $r_n = \dim \chi_m^n$ and $A_i = A_i A'_i$.
- 3) Normalisation: $M(K_{(m)A}^{(\ell)}) \geq \ell$.

Then the regularisation of the function M given by $M^\infty(P) = \limsup_{n \rightarrow \infty} \frac{M(P^{\otimes n})}{n}$ is an upper bound on $C_D^{(m)}$, i.e., $M^\infty(P_{(m)AA'}) \geq C_D^{(m)}(P_{(m)AA'})$ for all $P_{(m)AA'}$ with $\dim \chi_m^n < \infty$. If in addition M satisfies

4. Subadditivity on tensor products: $M(P^{\otimes n}) \leq nM(P)$, then M is an upper bound for $C_D^{(m)}$.

Proof. The proof of this theorem is in full analogy to that of the theorem 2 hence we do not present it here. It needs however the facts analogous to that from remark 1 which we present below.

We first argue, that the maximization in the definition of the distillable key $C_D^{(m)}$ can be taken over the protocols which have only linear amount of communication. To prove this, we observe, that the quantum multipartite Devetak-Winter (D-W) protocol provided in [13] can be applied also in the classical case, with appropriate change of quantum operations to classical data processing operations. Such modified quantum multipartite D-W protocol we will call a *classical multipartite D-W protocol*.

The quantum multipartite D-W protocol, as a multipartite extension of the Devetak-Winter protocol, works for multipartite ccq states. It is easy to see that is essentially classical i.e. can be done with help of local classical operations and public communication. Indeed, instead of quantum POVM's that are used by the honest parties in this protocol [35], [13], one can consider classical operations, that are based on the classical Slepian-Wolf theorem [14]. Moreover, if some amount of key can be obtained from the multipartite ccq state, then it can be also obtained from this state after projecting onto Eve's subsystem turning it into a classical state. For this reason, the classical multipartite D-W protocol applied to the probability distribution gains at least that much of secure key, as the quantum one. Since the quantum multipartite D-W protocol uses only a linear amount of communication, so will the classical one (see lemma 3).

We argue now, that the dimension of the ancillary system used to implement local operations in the classical multipartite D-W protocol is also linear in the number of input copies. This holds by the same property of the quantum D-W protocol, that has been noted in remark 2.

In summary, we have that the dimension of the output variable of the honest parties is only linear in the number of input copies. This ends the proof of the above theorem.

Remark 3 Note that from [12] it follows that the above theorem holds for a special class of distributions. These are distributions for which Eve's distribution is a function of Alice's and Bob's joint distribution. Unfortunately, one can not follow this approach to extend the results to all distributions. This is because there are distributions for which $C_D \neq K_D$. For this reason we can not use directly the "unified formalism" given in [12] to get the result.

Example 2 (multipartite intrinsic information as an upper bound on classical distillable key) We will show now, that there holds:

$$\frac{1}{(m-1)} I((m)A \downarrow E)_P \geq C_D^{(m)}(P), \quad (89)$$

where P is some distribution of variables $(m)A$. As in case of the multipartite squashed entanglement, we merely check that this function satisfies the axioms of the above theorem.

In what follows, we will not assume, that the multipartite intrinsic information is realized on a particular variable E , which seems however to be true due to it being true for the bipartite intrinsic information (see [36]).

Asymptotic continuity.— It is noted in [5], that the multipartite intrinsic information is simply continuous in its argument (a weaker condition than that of asymptotic continuity). The asymptotic continuity of this function follows from general result contained in proposition 2 of Ref. [8] as explained in the bipartite case in section V.B of [8] (see also [37]). The reason is the same as in the case of mixed convex roof: the operation of “arrowing” preserves asymptotic continuity, and the continuity of conditional multipartite information follows from the Fannes inequality [33].

Monotonicity.— The monotonicity of the multipartite intrinsic information for the case where Eve is in a product state with the honest parties is shown in [5]. It is also noted there that in the general case the monotonicity also holds and the proof is a direct generalization of the monotonicity proof they have provided, hence we just briefly sketch the idea, for completeness of presentation. To show monotonicity under local operations, it remains to rewrite the multipartite intrinsic information in terms of bipartite conditional mutual information and use the chain rule for the latter. Then, the data processing inequality assures that the function can not increase. To see that communication can not increase it either, it is enough to see that it can be rewritten as if only Eve had the communication. It is then clear that discarding such information can only increase the multipartite intrinsic information.

Normalization.— Since for the multipartite intrinsic information there is a representation given in Eq. (17), it is easy to see that on the ideal distribution $K_{(m)AE}^{\log d}$ it takes value:

$$I(K_{(m)A}^{\log d} | K_E^{\log d}) = \sum_{i=1}^m S(A_i) - S((m)A) = (m-1) \log d, \quad (90)$$

where d is the dimension of the support of A_1 . Hence, by theorem 4, we get that $\frac{1}{(m-1)} I((m)A \downarrow E) \geq C_D^{(m)}$.

Example 3 A similar result is true also for another monotone which is a version of S_m extended to $m+1$ systems which we denote following [5] as $S_m \downarrow$.

$$\begin{aligned} S_m \downarrow := & \inf_{E \rightarrow \bar{E}} [I(A_1 : A_2 \dots A_m | \bar{E}) \\ & + I(A_2 : A_3 \dots A_m | A_1 \bar{E}) + I(A_3 : A_4 \dots A_m | A_2 A_1 \bar{E}) \\ & + \dots + I(A_{m-1} : A_m | A_{m-2} \dots A_1 \bar{E})]. \end{aligned} \quad (91)$$

To get rid of the infimum, we realize $S_m \downarrow$ via the sequence of channels $E \rightarrow \bar{E}_n$. Then for each n we observe that each term as in the above sum is just a difference of mutual informations. E.g. $I(A_2 : A_3 \dots A_m | \bar{E}_n) = I(A_2 : A_3 \dots A_m | \bar{E}_n) - I(A_2 : \bar{E}_n | A_1)$, that forms a ‘pair’. It is then easy to see, that apart from the first such ‘pair’ which equals \log of the dimension of the support of A_1 , all the others are equal to zero. Hence we have that

$$S_m \downarrow \geq C_D^{(m)}. \quad (92)$$

VI. CONCLUSIONS

In summary, we present two new multipartite entanglement measures, the generalized q-squashed entanglement and the c-squashed one. There were obtained by squashing the conditional multipartite mutual information over the extension states (i.e. taking the infimum). When the ancilla register is quantum we get the q-squashed entanglement, and when it is classical we get the c-squashed one. Each measure has two versions corresponding to two possible multipartite mutual informations I and S_m . The q-squashed entanglements are additive, while for the c-squashed additivity is an open question.

Notice that we consider two types of correlation between the system and the ancilla in the extension states – completely quantum correlation and classical correlation. Suppose now that we allow only the extensions of the form $\sum p_i \rho_{A_1 \dots A_m}^i \otimes \phi_E^i$ where ϕ_E^i is an unnecessarily orthogonal states. That is we restrict the extension to separable states between the system and the ancilla. Is it still a good entanglement measure by squashing? The answer is yes. As a matter of fact, one can check that the proof of monotonicity of E_{sq}^q can be applied to any convex extension set. For example one can allow the extension to be *PPT* state between the system and the ancilla. We thus have a whole family of entanglement measures.

We have shown also, that any multipartite entanglement measure which satisfies reasonable axioms, is an upper bound on the multipartite distillable key K_D . Using this fact we proved that q-squashed entanglement is an upper bound on K_D . It is not difficult to see that the same holds for the regularized mixed convex roof of the function I_c . We also revisit the analogous result in the classical realm given in [5], addressing more carefully the issue of asymptotic continuity, as well as the presence of the eavesdropper.

Note added: After completing this manuscript we have noticed a paper by G.A. Paz-Silva and J.H. Reina, quant-ph/0702177, which also proposed a procedure to build entanglement measures based on mixed convex roof. Also, we have got to know, that Patrick Hayden and Ivan Savov have independently proposed a multipartite version of squashed entanglement.

Acknowledgements: The authors are grateful to the two anonymous referees for their detailed comments and suggestions that helped to improve the paper. M.H. would like to thank Piotr Badziąg for discussions. We gratefully thank the Newton Institute, Quantum Information Science 2004 where much of this work was completed.

REFERENCES

- [1] R. Tucci, “Entanglement of distillation and conditional mutual information,” ArXiv: quant-ph/0202144.
- [2] M. Christandl and A. Winter, “Squashed entanglements - an additive entanglement measure,” *J. Math. Phys.*, vol. 45, pp. 829, 2003.
- [3] G. Lindblad, “Entropy, information and quantum measurements,” *Commun. Math. Phys.*, vol. 33, pp. 111-119, 1973.
- [4] R. Horodecki, “Informationally coherent quantum systems,” *Phys. Lett. A*, vol. 187, pp. 145-150, 1993.
- [5] N. J. Cerf, S. Massar, and S. Schneider, “Multipartite classical and quantum secrecy monotones,” *Phys. Rev. A*, vol. 66, pp. 042309, 2002.
- [6] A. Uhlmann, “Entropy and optimal decompositions of states relative to a maximal commutative subalgebra,” *Open Sys. Inf. Dyn.*, vol. 5, pp. 209, 1998.

- [7] M. Christandl, *The Quantum Analog To Intrinsic Information*, Diploma Thesis, Institute for Theoretical Computer Science, ETH Zurich, 2002.
- [8] B. Synak-Radtke and M. Horodecki, "On asymptotic continuity of functions of quantum states," *J. Phys. A*, vol. 39, pp. L423, 2006.
- [9] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke, "Irreversibility for all bound entangled states," *Phys. Rev. Lett.* vol. 95, pp. 190501, 2005.
- [10] O. Nagel and G. Raggio, "Another state entanglement measure," ArXiv: quant-ph/0306024.
- [11] R. Alicki and M. Fannes, "Continuity of conditional quantum mutual information," *J. Phys. A*, vol. 37, pp. L55-L57, 2004.
- [12] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, "On distillation of classical key from quantum states," quant-ph/0608199.
- [13] R. Augusiak and P. Horodecki, "Multipartite Secret Key Distillation and Bound Entanglement," arXiv:0811.3603.
- [14] T. M. Cover and J. A. Thomas, *Elements of information theory*, Wiley, 1991.
- [15] G. Lindblad, "Completely positive maps and entropy inequalities," *Commun. Math. Phys.* vol. 40, pp. 147, 1975.
- [16] A. Uhlmann, "Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory," *Commun. Math. Phys.*, vol. 54, pp. 21-32, 1977.
- [17] M. Horodecki, J. Oppenheim, and A. Winter, "Partial quantum information," *Nature*, vol. 436, pp. 673, 2005.
- [18] M. Horodecki, "Simplifying monotonicity conditions for entanglement measures," *Open Sys. Inf. Dyn.*, vol. 12, pp. 231, 2005.
- [19] J. Oppenheim, "A paradigm for entanglement theory based on quantum communication," arXiv:0801.0458.
- [20] D. Avis, P. Hayden, and I. Savov, "Distributed compression and multi-party squashed entanglement," *J. Phys. A*, vol. 41, 2008.
- [21] M. A. Nielsen, "Continuity bounds on entanglement of formation," *Phys. Rev. A*, vol. 61, pp. 064301, 2000.
- [22] G. Vidal, "Entanglement monotones," *J. Mod. Opt.*, vol. 47, pp. 355, 2000.
- [23] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, "Locking classical correlations in quantum states," *Phys. Rev. Lett.*, vol. 92, pp. 067902, 2004.
- [24] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Locking entanglement with a single qubit," *Phys. Rev. Lett.*, vol. 94, pp. 200501, 2005.
- [25] R. Koenig, R. Renner, A. Bariska, and U. Maurer, "Locking of accessible information and implications for the security of quantum cryptography," *Phys. Rev. Lett.*, vol. 98, pp. 140502, 2007.
- [26] M. Christandl and A. Winter, "Uncertainty, monogamy, and locking of quantum correlations," *IEEE Trans. Inf. Theory*, vol. 51, 2005.
- [27] F. Brandao, *Entanglement Theory and the Quantum Simulation of Many-Body Physics*, Ph.D. thesis, Imperial College, 2008.
- [28] M. Christandl, *The Structure of Bipartite Quantum States - Insights from Group Theory and Cryptography*, Ph.D. thesis, University of Cambridge, 2006.
- [29] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 773, 1993.
- [30] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355, 1975.
- [31] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339348, 1978.
- [32] P. Horodecki and R. Augusiak, "Quantum states representing perfectly secure bits are always distillable," ArXiv: quant-ph/0602176.
- [33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
- [34] M. Fannes, "A continuity property of the entropy density for spin lattice systems," *Commun. Math. Phys.*, vol. 31, 1973.
- [35] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. R. Soc. Lond. A*, vol. 461, 2005.
- [36] M. Christandl, R. Renner and S. Wolf, "A property of the intrinsic mutual information," in *International Symposium on Information Theory (ISIT)*, 2003.
- [37] R. Renner and S. Wolf, "New bounds in secret-key agreement: the gap between formation and secrecy extraction," *Advances in Cryptology - EUROCRYPT '03, Lecture Notes in Computer Science* Springer-Verlag, 2003.

Dong Yang received his Ph.D. in Physics from Zhejiang University in 2002. He joined the Laboratory of Quantum Information at China Jiliang University in June 2007. Currently his research interests include quantum information theory, entanglement theory, and quantum computation.

Karol Horodecki graduated from University of Gdańsk, Gdańsk, Poland, in 2004, where he is currently teaching assistant at the Institute of Informatics, having received the Ph.D. degree in computer science from the University of Warsaw in 2009. He is a coauthor of several papers on processing of quantum information. His research interests are in quantum information theory.

Michał Horodecki graduated from University of Gdańsk, Gdańsk, Poland, in 1997 and received the Ph.D. degree in physics from the same university in 2000. In 2007, he was appointed Professor at the University of Gdańsk. He is a coauthor of Quantum Information (New York: Springer-Verlag, 2001). His main achievements include pioneering research on the entanglement of mixed states, in particular, bound entanglement and quantum state merging. His research interests are in quantum information theory and the foundations of quantum physics.

Paweł Horodecki graduated from University of Gdańsk, Gdańsk, Poland, in 1995 and received the Ph.D. degree in physics from the Technical University of Gdańsk, Gdańsk, Poland, in 1999. In 2008, he became a Professor at the Technical University of Gdańsk. He is a coauthor of Quantum Information (New York: Springer-Verlag, 2001). His main achievements include pioneering research on the entanglement of mixed states, in particular, bound entanglement. His research interests are in quantum information theory and foundations of quantum physics.

Jonathan Oppenheim graduated from the University of Toronto, Toronto, ON, Canada, in 1993, and received the Ph.D. degree under B. Unruh from the University of British Columbia, Vancouver, BC, Canada, in 2001. Currently, he is Royal Society University Research Fellow at the Department of Applied Mathematics and Theoretical Physics (DAMTP), University of Cambridge, Cambridge, U.K. His research interests include quantum information theory, foundations of quantum mechanics, quantum gravity, and black hole thermodynamics.

Wei Song received his Ph.D. in Physics from the University of Science and Technology of China in 2008. Currently he works as a Lecturer in the School of Physics and Telecommunication Engineering of the South China Normal University. His research interests include various aspects of quantum information science and quantum simulation in condensed matter physics.